PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-232963

(43)Date of publication of application : 16.08.2002

---

(51)Int.Cl. H04Q 7/38

G08B 13/196

G08B 25/00

G08B 25/04

G08B 25/10

// H04L 9/10

---

(21)Application number : 2001-059216 (71)Applicant : LAUREL

INTELLIGENT SYSTEMS CO LTD

(22)Date of filing : 29.01.2001 (72)Inventor : TORIKAI MASAMICHI

FUJII MIKIO

UGAI TAKESHI

---

(54) SECURITY MAINTENANCE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system where notice on the occurrence of a fault, transmission by an image, storage on the occurrence of the fault, and access to the image can properly be executed and leakage of information to other than concerned people is not cared about.

SOLUTION: An image picked up by a digital image pickup camera and encrypted is stored, transmitted to a personal computer, a mobile phone or a mobile information terminal, the encrypted image is decoded by a removable decoding key device and the image is confirmed, thus leakage of the image information is not cared about.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The system which it memorizes to storage where the image picturized with the camera which can be picturized by the digital image interlocked with the sensor with the signal of a sensor is enciphered, and this is made into ready-for-sending ability at a personal computer, a portable telephone, or a portable information terminal, and can be decrypted at a personal computer, a portable telephone, or a portable information terminal [claim 2] making a decryption possible with decryption key devices which consist of a personal computer and a portable telephone or a CPU that desorption was possible to the portable information terminal, and stored key information required for encryption and a decryption in it, a memory chip, etc. in a system according to claim 1, such as a key stick and an IC card, -- [claim 3] Thing [claim 4] in a system according to claim 1, encipher the picturized image, register with a server's homepage, and accessible at a personal computer, a portable telephone, and a portable

information terminal Thing [claim 5] which it is at the generating time of a detecting signal, and enciphers the image picturized before it and is memorized to storage in a system according to claim 1 Thing [claim 6] which enciphers after compression of an image in a system according to claim 1 transmitting the image newly picturized for every fixed time amount from the time of generating of a detection signal from a server to a personal computer and a portable telephone, or a portable information terminal in a system according to claim 1 -- [claim 7] It is [independent or] using together and using about what detects vibration, a sound, various beams of light, the MAG, temperature, smoke, etc. in a sensor in a system according to claim 1.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the approach of transmitting a personal computer, a portable telephone, or the image enciphered to the portable information terminal while enciphering and memorizing the image which used and picturized digital image pick-up cameras (CCD camera etc.) at the time

of the malfunction detection signal generation from a malfunction detection sensor.

[0002]

[Description of the Prior Art] The abnormality detection sensor and this by the infrared radiation installed in current, an entrance, etc. are interlocked with, it has a digital image pick-up camera, and the equipment which looks at the image at the time of abnormalities with the personal computer connected to this is put in practical use in the system which the infrared radiation emitted by the body is detected [system] and operates a digital image pick-up camera. On the other hand, the technique of transmitting an image between portable telephones or between a server and a portable telephone is put in practical use.

[0003]

[Problem(s) to be Solved by the Invention] A private part may be picturized, when an image pick-up may always be performed and it installs the image picturized with a digital image pick-up camera in ordinary homes. As for the picturized image, it becomes [anyone] infringement of privacy about this and is not desirable a portable telephone and to access at a personal computer and to see. Moreover, the storage of the picturized image may be copied or it may be abused [may be and] for a theft. The current system is defenseless about leakage of image information. Notice at the time of an abnormal occurrence,

transmission by the image and the storage at the time of abnormalities, and access to an image are performed appropriately, and the anxious system of an information leak which is not is called for in addition to the persons concerned.

[0004]

[Means for Solving the Problem] About this design, the reduced screen doubled with the screen size of a portable telephone or a portable information terminal with the server by which the image picturized with the digital image pick-up camera for an abnormality monitor is connected to this with the signal from abnormality detection sensors, such as an infrared sensor which detects a trespasser etc., is created, and while carrying out an extraordinary call at coincidence, this image is transmitted to two or more sets of the portable telephones registered beforehand, and a portable information terminal.

[0005] The image captured by the server is transmitted one after another (for example, 3-second spacing) for every fixed time amount. At the portable telephone which received the extraordinary call, or a portable information terminal, the screen at the time of abnormalities can be continuously seen on a portable telephone or the display of a portable information terminal by the click of an actuation key, and the situation of a site can be grasped. On the other hand, except creating the still picture for transmission for every fixed time amount which captured the image in the state of [camera / digital image pick-up] the

animation, and was described above, after receiving the signal of abnormality detection, with dynamic-image compression means, such as MPEG, an image is compressed about into 1/10, it enciphers after that, and a server captures the image of incorporation size to the storage in a server.

[0006] An image can be downloaded in two or more personal computers connected to the server by LAN, and can be seen as a detail image. Only those who have at this the decryption key device in which desorption is possible in a personal computer are able to see. generating of an abnormality signal or before -- or after resetting, a server always incorporates, compresses, enciphers and memorizes an animation from a digital image pick-up camera. An infrared camera is used in a dark location. Although this image is memorized by the storage with fixed storage capacity, when a storage is saturated, it is overwritten by the image new at any time sequentially from the image memorized previously. The whole of this image is moved to generating and coincidence of an abnormality signal by another storage area. Since the image of fixed time amount before this malfunction detection can check the situation to an abnormal occurrence, status tracking at the time of abnormalities can be appropriately performed with an image after the birth [from abnormalities]. Even if the storage of a personal computer or a server is in a theft, the image which an image does not have worries about leakage since it is enciphered, and is transmitted to a

cellular phone or a portable information terminal is not enciphered, but since transmission is restricted to what was registered beforehand, it does not have a fear of information leaking.

[0007] It can be made to perform incorporation of an image by, uploading to a server the image captured from the digital image pick-up camera as another means on the other hand, registering with the homepage which created in the server two kinds of images enciphered as what was enciphered after contraction image creation after compressing the image of incorporation size, and downloading from a homepage at a personal computer and a portable telephone, or a portable information terminal. Since an image can be decrypted by equipping a personal computer and a portable telephone, or a portable information terminal with the decryption key in which desorption is possible, much more security protection becomes possible.

[0008]

[The gestalt of invention implementation] This design is explained to a detail using drawing. Drawing 1 shows the structure of a system of this design. The sensor by which 1 detects an invader in drawing 1 , the digital image pick-up camera installed as an invader gone into a field of view in 2, The light from which, as for 3, the quantity of light changes by the sensor, and 4 capture an image. Compression processing, The server which has functions, such as encryption

processing, image storage, and image transmission, The personal computer to which 5 is connected to a server with the authentication key device for server grabbing, and 6 is connected by LAN, the decryption key device by which 7 is connected to the USB terminal of a personal computer etc., and 8 -- a portable telephone (a cellular phone --) For generic names, such as PHS and J-Phone, or a portable information terminal, and 9, as for the line network of a portable telephone or a portable information terminal, and 11, a portable telephone or the decryption key device for portable information terminals, and 10 are [LAN and 12] monitor fields.

[0009] Drawing 2 shows actuation of this system with a flow chart. It explains along with a flow chart. In the usual condition until the detection sensor 1 operates, an image is captured in a server 4 as a dynamic image with the digital image pick-up camera 2. By dynamic-image compression means, such as MPEG, it is compressed about into 1/10, it is enciphered, and the captured image is memorized by the storage. This image can be downloaded with two or more personal computers 6 connected by LAN of 11, and can always be seen. Since it is enciphered, an image elongates [insert it in the USB terminal of a personal computer etc., it decrypts it, and] and looks at the decryption key 7. The capacity of a storage is decided, and when saturated, the image of fixed time amount (for example, 10 minutes) is always memorized by overwriting

sequentially from the direction of an old image. In a dark location, if the quantity of light of a light is controlled by the photosensor using an infrared camera, it can picturize, without being noticed by the illegal permeation person etc.

[0010] It is usually transmitted to another record area in a server 4 at the time of actuation of a sensor 1, with [above] the image at the time enciphered. A new image is captured in a server and the contraction image of the still picture set by the screen size of a portable telephone or the portable information terminal 8 is created. Creation of a contraction image is performed for every fixed time amount. It calls at two or more portable telephones registered or the portable information terminal 8, and an image is transmitted. At a portable telephone or the portable information terminal 8, the still picture sent for every fixed time amount by the click of an actuation key can be seen one after another.

[0011] On the other hand, with incorporation size, it is compressed and enciphered and the picturized image is memorized in the work area in a server 4. Since it can download in the personal computer 6 connected to the server 4 by LAN11, the decryption key device 7 can be inserted in the UBS terminal of a personal computer etc., it can decrypt and elongate and it can see as a detail image, an outline can be grasped by the image of a portable telephone or the portable information terminal 8, and a detail image can be checked with a personal computer if needed.

[0012] It is also possible to download and compare the image before and behind sensor 1 actuation with a personal computer. The exposure time after a sensor 1 operates is defined with equipment. (For example, 10 minutes) The image before sensor 1 actuation and the image recording after actuation can be used also as an image of the proof to the police etc. later.

[00013] As for drawing 2 , drawing 3 shows an option. A homepage is created to a server 4 and the captured image is registered into him. The image to register is three kinds of prior images compressed and enciphered in the image compressed and enciphered in the thing and incorporation size which enciphered the image of a portable screen size, and incorporation size. These images can see an image by downloading from a server's homepage, respectively with a portable telephone, the portable information terminal 8, or a personal computer 6.

[0014] In this case, since the image downloaded to the portable telephone or the portable information terminal 8 is also enciphered unlike the case of drawing 2 , a decryption key device is inserted and decrypted into the slot for decryption key device 9 insertion prepared in the portable information terminal 8. If it does in this way, it is more desirable than a security-protection top from the approach shown in drawing 2 .

[0015] Since an image with clearer incorporating with a still picture depending on

the digital image pick-up camera 2 is obtained, a compression method uses JPEG etc. in this case, the method which takes in a static image for every fixed time amount instead of a dynamic image may be used, and the approach of incorporating with a static image, processing and changing with a dynamic image after transmission is [moreover it compresses about into 1/30, incorporation of a static image and incorporation of a dynamic image are changed, and] also on the other hand, effective at first.

[0016] The cryptographic algorithm currently introduced by JP,6-102822,A is used for encryption. This cipher system consists of the combination of for example, the EKUSU crew sheave OR, a cutting tool permutation, and substitution, and it is characterized by a batch being a variable-length cutting tool. Thereby, picture transmission with difficult decode becomes possible at high speed. Moreover, this algorithm is a method which enciphers an image using the cryptographic key information stored in the cryptographic key device. It is usable, if decode at a high speed is difficult even if it is other algorithms.

[0017] Moreover, about this design, encryption of an image is performed after compression of an image for improvement in the speed of cipher processing. The decryption key device 7 is inserted in the USB terminal of a personal computer 6, it decrypts by the same processing as the case where it enciphers using the data code key information stored in this, and a decryption is also

displayed after expanding of data. For this reason, it enables only the decryption key device 7 or the owner of 9 to see an image.

[0018] Moreover, it becomes the system which can use it as preventing trespass, i.e., crime prevention, and can also perform an image check by preparing an extraordinary bell etc., although there is nothing to a light 3 and drawing, making the quantity of light increase with the signal of a sensor 1, or sounding an alarm bell.

[0019] If a therms sensor, a smoke sensing sensor, vibration, the sensing sensor of a sound, etc. are used for a sensor 1 other than an infrared sensor or it uses together, the fire at the time of absence and the situation in case of an earthquake can also check a situation by the image of a portable telephone or the portable information terminal 8.

[0020] Even if the power is turned off by the server 4, it has a backup power supply by the dc-battery so that this system may carry out a fixed time amount function.

[0021] Moreover, it is [OFF / of a server power source] operational only in the holder of the authentication key device 5.

[0022]

[Effect of the Invention] According to the security maintenance system of this design, since the image picturized with the digital image pick-up camera is

enciphered and memorized, those who decrypt this and can be seen are restricted to people with a decryption key. Since it limits to a portable telephone, the portable telephone of specification [the image transmitted to a portable information terminal], or a portable information terminal or leakage control of image information is further made perfect, a portable telephone or the transmitting image to a portable information terminal can also be enciphered. Conventionally, a private scene may be picturized depending on the location installed, and the system which has the camera of an abnormality monitor had accessible others in this remaining as record. Although the function of a system is improving by the spread of a computer or portable telephones, on the other hand, the problem of leakage of secrets is an important technical problem. About this design, this technical problem is solved, and a system can be installed in comfort. At the time of an abnormal occurrence, the situation of a site can be promptly grasped by the image with a portable telephone or a portable information terminal, and the detail image before abnormality detection and after detection and an animation can be checked with a personal computer. Moreover, even if normal, the situation of a site can sometimes be grasped at a portable telephone or a portable information terminal from a remote place. The record image is important also as a presentation proof to the police.

[0023]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a security maintenance structure-of-a-system Fig.

[Drawing 2] The thing in the case of transmitting without enciphering an image to a portable telephone or a portable information terminal in drawing having shown the sequence of this system actuation.

[Drawing 3] The thing in the case of enciphering an image also to a portable telephone or a portable information terminal, and transmitting to it in drawing having shown the sequence of this system actuation.

[0024]

[Description of Notations]

1 Sensor for Invader Detection

2 Digital Image Pick-up Camera (Image Pick-up of Animation and Still Picture is Possible in Digital One, Such as CCD Camera)

3 Light from which Quantity of Light Changes by Sensor

4 Server

5 Authentication Key Device for Server Grabbing

6 Personal Computer

7 Decryption Key Device (for Personal Computers) : Key Stick, IC Card, Etc. Which Consist of a CPU Which Stored Key Information Required for Encryption and Decryption, a Memory Chip, Etc.

8 Portable Telephone: (Cellular Phone, PHS, J-Phone, Etc.) or Portable Information Terminal (it is Terminal in which Image Display is Possible by Communication Link)

9 Decryption Key Device (Portable Telephone or for Portable Information Terminals) : Key Stick, IC Card, Etc. Which Consist of a CPU Which Stored Key Information Required for Encryption and Decryption, a Memory Chip, Etc.

10 Line Network of Portable Telephone or Portable Information Terminal

11 LAN

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－232963
（P2002－232963A）
(43)公開日　平成14年８月16日(2002.8.16)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｈ０４Ｑ　7/38		Ｇ０８Ｂ　13/196		５Ｃ０８４
Ｇ０８Ｂ　13/196			25/00　５１０Ｍ	５Ｃ０８７
25/00	５１０		25/04　Ｇ	５Ｊ１０４
25/04			25/10　Ｄ	５Ｋ０６７
25/10		Ｈ０４Ｂ　7/26	１０９Ｒ	

審査請求　未請求　請求項の数７　書面　（全　６　頁）　最終頁に続く

(21)出願番号　特願2001－59216(P2001－59216)

(22)出願日　平成13年１月29日(2001.1.29)

(71)出願人　591234204
株式会社ローレルインテリジェントシステムズ
神奈川県横浜市青葉区美しが丘５丁目35番地の２

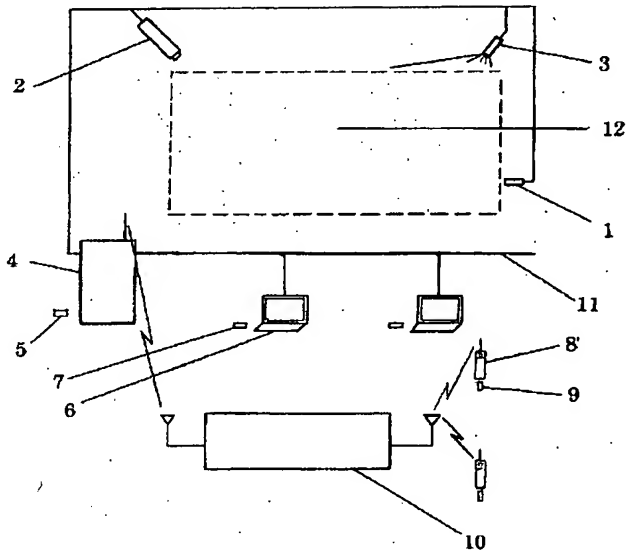
(72)発明者　鳥飼　将迪
神奈川県横浜市青葉区美しが丘５丁目35番地の２　株式会社ローレルインテリジェントシステムズ内

(72)発明者　藤井　幹雄
神奈川県横浜市青葉区美しが丘５丁目35番地の２　株式会社ローレルインテリジェントシステムズ内

最終頁に続く

(54)【発明の名称】　保安維持システム

(57)【要約】
【課題】不法侵入者などをセンサーで検知し、連動したデジタル撮像カメラで撮影し、携帯電話、または携帯用情報端末の画像及びパソコンで状況を確認確認、記録するシステムで画像情報の漏洩に関して無防備である。
【解決手段】デジタル撮像カメラで撮像された画像を暗号化した状態で記憶し、パソコンや携帯用電話、または携帯用情報端末に伝送し、これらに脱着可能な復号化キーデバイスで復号化し、画像の確認を行うので画像情報が漏れる心配はない。



【特許請求の範囲】
【請求項１】センサーの信号により、センサーに連動したデジタル画像で撮像可能なカメラにより撮像された画像を暗号化した状態で記憶装置に記憶し、これをパソコン、携帯用電話、または携帯用情報端末に送信可能とし、パソコン、携帯用電話、または携帯用情報端末で復号化することが可能なシステム
【請求項２】請求項１に記載のシステムにおいて、パソコン及び携帯用電話、または携帯用情報端末に脱着可能で暗号化及び復号化に必要なキー情報を収めたＣＰＵ、メモリーチップ等で構成されるキースティツク、ＩＣカードなどの復号化キーデバイスにより復号化を可能にすること
【請求項３】請求項１に記載のシステムにおいて、撮像された画像を暗号化してサーバーのホームページに登録し、パソコン及び携帯用電話及び携帯用情報端末でアクセス可能であること
【請求項４】請求項１に記載のシステムにおいて、検出信号の発生時点で、それ以前に撮像された画像を暗号化し、記憶装置に記憶すること
【請求項５】請求項１に記載のシステムにおいて暗号化を画像の圧縮後に行うこと
【請求項６】請求項１に記載のシステムにおいて、検知信号の発生時から一定時間毎に新しく撮像された画像をサーバーからパソコン及び、携帯用電話、または携帯用情報端末に送信すること
【請求項７】請求項１に記載のシステムにおいてセンサーに振動、音、各種光線、磁気、温度、煙などを検知するものを単独または、併用して用いること
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は異常検出センサーからの異常検出信号発生時にデジタル撮像カメラ（ＣＣＤカメラなど）を用いて撮像した画像を暗号化して記憶すると共に、パソコン、、携帯用電話または、携帯用情報端末に暗号化した画像を送信する方法に関する。
【０００２】
【従来の技術】現在、出入り口等に設置される赤外線による異常検知センサーとこれに連動しデジタル撮像カメラを有し、人体から発する赤外線を検知してデジタル撮像カメラを作動させるシステムにおいて、これに接続されたパソコンで異常時の画像を見る装置が実用化されている。一方、携帯用電話間、またはサーバーと携帯用電話間に画像を送信する技術が実用化されている。
【０００３】
【発明が解決しようとする課題】デジタル撮像カメラで撮像する画像は常時撮像が行われる場合もあり、一般家庭に設置する場合などは、プライベートな部分が撮像されることもある。撮像された画像は、これを誰でも携帯用電話や、パソコンにアクセスして見られることはプライバシイの侵害になり好ましくない。また、撮像した画像の記憶装置がコピーされたり、盗難にあって悪用されることもある。現在のシステムは画像情報の漏洩に関しては無防備である。異常発生時の通知や、画像による伝送、異常時の記憶、画像へのアクセスが適切に行われ、かつ、関係者以外に情報漏洩の心配のないシステムが求められる。
【０００４】
【課題を解決するための手段】本考案では不法侵入者などを検知する赤外線センサーなどの異常検知センサーからの信号により、異常監視用のデジタル撮像カメラで撮像された画像をこれに接続されるサーバーで携帯用電話、または携帯用情報端末の画面サイズに合わせた縮小画面を作成し、あらかじめ登録されている複数台の携帯用電話、または携帯用情報端末に同時に非常コールするとともにこの画像を送信する。
【０００５】サーバーに取り込まれた画像は一定時間毎に（例えば３秒間隔）次々に送信される。非常コールを受けた携帯用電話、または携帯用情報端末では操作キーのクリックで異常時の画面を携帯用電話、または携帯用情報端末のディスプレイで連続的に見ることが出来、現場の状況を把握する事が出来る。一方、サーバーは異常検知の信号を受けてから動画の状態でデジタル撮像カメラより画像を取り込み、上記した一定時間毎に送信用の静止画を作成する以外は取り込みサイズの画像をＭＰＥＧなどの動画像圧縮手段により、１／１０程度に画像を圧縮し、その後暗号化してサーバー内の記憶装置に取り込む。
【０００６】画像はサーバーにＬＡＮで接続されている複数台のパソコンにダウンロードして詳細画像として見ることが出来る。これにはパソコンに脱着可能な復号化キーデバイスを持つ人のみ見ることが可能である。異常信号の発生以前、または、リセットしてからは、サーバーは常時動画をデジタル撮像カメラから取り込んで圧縮し、暗号化して記憶する。暗い場所では暗視カメラを使用する。この画像は一定の記憶容量を持つ記憶媒体に記憶されるが、記憶媒体が飽和した場合、先に記憶した画像から順に随時新しい画像に上書きされる。異常信号の発生と同時にこの画像はすべて別の記憶エリアに移される。この異常検出前の一定時間の画像は異常発生までの状況を確認出来るので、異常発生後の画像と共に異常時の状況把握を適切に行うことが出来る。パソコンやサーバーの記憶装置が盗難にあっても画像は暗号化されているので漏洩の心配もなく、また、携帯電話、または携帯用情報端末に送信される画像は暗号化されていないが、送信はあらかじめ登録したものに限られるため情報が漏れる心配がない。
【０００７】一方、もう一つの手段としてデジタル撮像カメラから取り込んだ画像をサーバーにアップロードし、縮小画像作成後暗号化したものと、取り込みサイズ

の画像を圧縮後暗号化した二種類の画像をサーバー内に作成したホームページに登録し、パソコン及び携帯用電話、または携帯用情報端末でホームページからダウンロードすることにより、画像の取り込みが出来るようにする。パソコン及び携帯用電話、または携帯用情報端末に脱着可能な復号化キーを装着することで画像を復号化出来るので、より一層の機密保持が可能となる。

【０００８】

【発明実施の形態】本考案を図を用いて詳細に説明する。図１は本考案のシステムの構成を示す。図１において１は侵入者を検知するセンサー、２は侵入者を視界に入るように設置されたデジタル撮像カメラ、３はセンサーで光量が変化するライト、４は画像を取り込み、圧縮処理、暗号化処理、画像記憶、及び画像送信、などの機能を有するサーバー、５はサーバー操作の為の認証キーデバイス、６はサーバーにＬＡＮで接続されているパソコン、７はパソコンのＵＳＢ端子などに接続される復号化キーデバイス、８は携帯用電話で（携帯電話、ＰＨＳ、Ｊ－フォンなどの総称）、または携帯用情報端末、９は携帯用電話、または携帯用情報端末用復号化キーデバイス、１０は携帯用電話、または携帯用情報端末の回線網、１１はＬＡＮ、１２は監視領域である。

【０００９】図２はこのシステムの作動をフローチャートで示したものである。フローチャートに沿って説明する。検知センサー１が作動するまでの通常の状態では画像はデジタル撮像カメラ２により動画像としてサーバー４内に取り込まれる。取り込まれた画像はＭＰＥＧなどの動画像圧縮手段により、１／１０程度に圧縮され、暗号化されて記憶媒体に記憶される。この画像は１１のＬＡＮで接続されている複数のパソコン６でダウンロードして常時見ることが出来る。画像は暗号化されているので復号化キー７をパソコンのＵＳＢ端子などに挿入し、復号化し、伸長して見る。記憶媒体の容量は決めておき、飽和した場合は古い画像の方から順に上書きをすることにより常に一定時間（例えば１０分）の画像を記憶する。暗い場所では暗視カメラを用い、光センサーによりライトの光量を制御すれば、不法浸入者などに気づかれずに撮像が可能である。

【００１０】センサー１の作動時は上記の通常時の画像は暗号化したままサーバー４内の別の記録エリアに転送される。新たな画像をサーバー内に取り込み、携帯用電話、または携帯用情報端末８の画面サイズに合わせた静止画の縮小画像を作成する。縮小画像の作成は一定時間毎に行われる。登録されている複数の携帯用電話、または携帯用情報端末８にコールをし、画像を送信する。携帯用電話、または携帯用情報端末８では、操作キーのクリックで一定時間毎に送られてくる静止画を次々に見る事が出来る。

【００１１】一方、撮像された画像は取り込みサイズのままサーバー４内のワークエリアで圧縮、暗号化され、記憶される。サーバー４にＬＡＮ１１で接続されているパソコン６にダウンロードし、復号化キーデバイス７をパソコンのＵＢＳ端子などに挿入し、復号化、伸長して詳細画像として見ることが出来るので、携帯用電話、または携帯用情報端末８の画像で概要を把握し、必要に応じてパソコンで詳細画像を確認する事が出来る。

【００１２】センサー１作動前後の画像をパソコンにダウンロードして比較することも可能である。センサー１が作動してからの撮影時間は装置により定める。（例えば１０分）後日、センサー１作動前の画像、作動後の画像記録は警察などへの証拠の画像としても使用できる。

【００１３】図３は、図２とは別の方法を示したものである。サーバー４にホームページを作成し、取り込んだ画像を登録する。登録する画像は携帯用画面サイズの画像を暗号化したもの、取り込みサイズで圧縮、暗号化した画像、及び取り込みサイズで圧縮、暗号化した事前画像の３種類である。これらの画像は携帯用電話、または携帯用情報端末８、またはパソコン６でサーバーのホームページからそれぞれダウンロードすることにより、画像を見ることが出来る。

【００１４】この場合、図２の場合と異なり、携帯用電話、または携帯用情報端末８にダウンロードした画像も暗号化されているので携帯用情報端末８に設けられた復号化キーデバイス９挿入用のスロットに復号化キーデバイスを挿入し復号化する。このようにすれば図２に示した方法より機密保持上より好ましい。

【００１５】一方、デジタル撮像カメラ２によっては静止画で取り込んだ方がより鮮明な画像が得られるので、動画像のかわりに静止画像を一定時間ごとに取り入れる方式でも良く、この場合、圧縮方式はＪＰＥＧなどを使用し、１／３０程度に圧縮する、また、静止画像の取り込みと動画像の取り込みを切り替え、最初は静止画像で取り込んで処理し、送信後に動画像に切りかえる方法も有効である。

【００１６】暗号化には、例えば特開平６－１０２８２２で紹介されている暗号アルゴリズムを使用する。この暗号方式は例えばエクスクルーシーブＯＲ、バイト置換、換字の組合わせから成り、処理単位が可変長バイトであることを特徴とする。これにより、高速で解読困難な画像伝送が可能となる。また、同アルゴリズムは暗号化キーデバイスに格納されている暗号化キー情報を使用して画像の暗号化を行う方式である。他のアルゴリズムであっても高速で解読困難なものであれば使用可能である。

【００１７】また、本考案では画像の暗号化は暗号処理の高速化のため、画像の圧縮後に行なわれる。復号化もパソコン６のＵＳＢ端子に復号化キーデバイス７を挿入し、これに格納されているデータ暗号キー情報により暗号化した場合と同様の処理により復号化し、データの伸長後表示する。このため復号化キーデバイス７又は９の

所有者のみ画像を見る事が可能となる。

【００１８】また、ライト３、図にはないが非常ベル等を設け、センサー１の信号により光量を増加させたり、または警鐘を鳴らすことにより、不法侵入を防ぐこと、即ち、防犯として使用出来、且つ、画像確認も出来るシステムとなる。

【００１９】センサー１には赤外線センサーの他に感温センサー、煙感知センサー、振動、音の感知センサーなどを使用したり、または、併用すると留守の時の火災、地震時の状況も携帯用電話、または携帯用情報端末８の画像で状況を確認することが出来る。

【００２０】サーバー４には電源が切られてもこのシステムが一定時間機能するようにバッテリーによるバックアップ電源を持つ。

【００２１】また、サーバー電源のＯＦＦは認証キーデバイス５の保持者のみが操作可能である。

【００２２】

【発明の効果】本考案の保安維持システムによれば、デジタル撮像カメラで撮像された画像は暗号化されて記憶されるのでこれを復号化して見れる人は復号化キーを持つ人に限られる。携帯用電話、または携帯用情報端末に送信される画像も特定の携帯用電話、または携帯用情報端末に限定するか、更に画像情報の漏洩防止を完全にする為、携帯用電話、又は携帯用情報端末への送信画像も暗号化することも出来る。従来、異常監視のカメラを有するシステムは設置される場所によってはプライベートな場面が撮像される場合があり、これが記録として残ったり、他人がアクセス可能であった。コンピューターや携帯用電話の普及により、システムの機能は向上しているが、反面、機密漏洩の問題は重要な課題である。本考案ではこの課題を解決し、安心してシステムを設置することが出来る。異常発生時には携帯用電話、または携帯用情報端末でいち早く画像で現場の様子を把握出来、異常検知前及び、検知後の詳細画像、動画をパソコンで確認することが出来る。また、異常がなくても、遠隔地から時々現場の様子を携帯用電話、または携帯用情報端末で把握することが出来る。記録画像は警察への提出証拠としても重要である。

【００２３】

【図面の簡単な説明】

【図１】保安維持システムの構成図である。

【図２】本システム作動の順序を示した図で携帯用電話、または携帯用情報端末には画像を暗号化しないで送信する場合のもの。

【図３】本システム作動の順序を示した図で携帯用電話、または携帯用情報端末にも画像を暗号化して送信する場合のもの。

【００２４】

【符号の説明】

１　侵入者検出のためのセンサー

２　デジタル撮像カメラ（ＣＣＤカメラなどのデジタルで動画及び静止画の撮像が可能なもの）

３　センサーで光量が変化するライト

４　サーバー

５　サーバー操作の為の認証キーデバイス

６　パソコン

７　復号化キーデバイス（パソコン用）：暗号化及び復号化に必要なキー情報を収めたＣＰＵ，メモリーチップ等で構成されるキースティツク、ＩＣカードなど

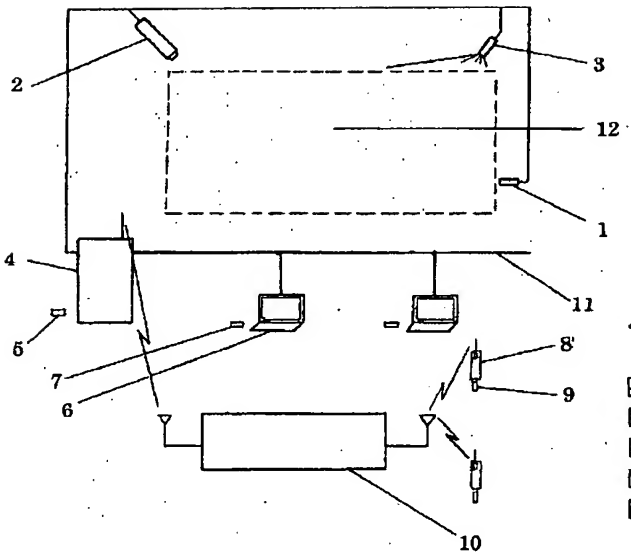
８　携帯用電話：（携帯電話、ＰＨＳ、Ｊ－フォンなど）又は、携帯用情報端末（通信で画像表示が可能な端末）

９　復号化キーデバイス（携帯用電話、または携帯用情報端末用）：暗号化及び復号化に必要なキー情報を収めたＣＰＵ，メモリーチップ等で構成されるキースティツク、ＩＣカードなど

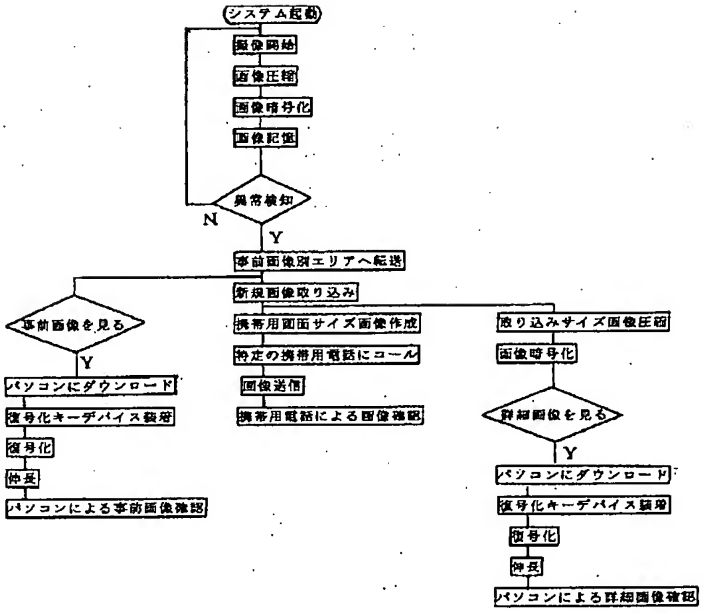
１０　携帯用電話、または携帯用情報端末の回線網

１１　ＬＡＮ

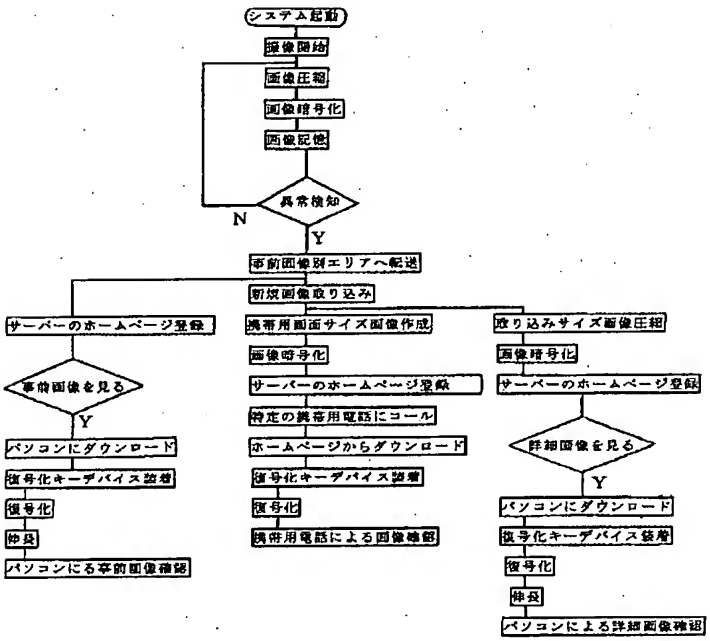
【図１】



【図２】



【図３】



フロントページの続き

(51)Int.Cl.⁷	識別記号	F I	ﾃｰﾏｺｰﾄﾞ（参考）
// Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ｚ

(72)発明者　鵜養　剛
神奈川県横浜市青葉区美しが丘５丁目35番地の２　株式会社ローレルインテリジェントシステムズ内

Ｆターム(参考)　5C084 AA02 AA07 AA13 BB33 BB40 CC17 DD11 EE01 EE03 EE04 FF02 FF04 FF27 GG07 GG09 GG43 GG52 GG78 HH10 HH12 HH13
5C087 AA22 AA24 AA25 BB03 BB12 BB18 BB74 DD05 DD23 DD24 EE05 EE16 EE20 FF01 FF02 FF04 FF17 FF19 FF20 GG02 GG12 GG18 GG23 GG32 GG66 GG67 GG70 GG83
5J104 AA04 AA12 AA16 AA18 AA19 EA04 NA02 NA09 NA10 NA35 NA37 NA41 PA02 PA07
5K067 AA30 BB04 BB21 DD52 FF23 HH23 HH36 KK13 KK15